CLAIM AMENDMENTS

Please amend the claims by canceling claims 5, 16 and 18-22, amending claims 4, 7 and 24, all without prejudice, as indicated on the following listing of all the claims in the present application after this Amendment:

1. - 3. (Canceled)

4. (Currently Amended) A computer readable storage medium having an executable program, the program to be utilized in an audio and/or video device for playback of encrypted audio and/or video files, the program configured to:

decrypt encrypted audio and/or video content of the file from a memory card based on a command received from a user interface of the device, wherein decrypting the audio or video content comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device;

copying a fractional portion of encrypted audio or video content of the file, the fractional portion comprising less than about 10 seconds of content of the file, from the memory card into a memory buffer of the device;

decrypting one or more of the copied encrypted keys;

decrypting the fractional portion of copied encrypted audio or video content of the file with the one or more decrypted keys; and

immediately deleting the one or more decrypted keys after decrypting the audio and/or video content before decrypting an additional fractional portion of content of the file.

5. (Canceled)

6. (Original) The software program of claim 4, wherein about two seconds of content is decrypted at a time with the one or more decrypted keys before the one or more keys are deleted.

7. (Currently Amended) A computer readable storage medium having an executable program, the program to be utilized in an audio and/or video device for playback of encrypted audio and/or video content, the program configured to:

decrypt an encrypted audio or video track from the memory card,

wherein decrypting the audio or video track comprises:

(a) calculating a media unique key; and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames comprising a portion of the track less than the entire track; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed.

8. - 22. (Canceled)

23. (Original) A system enabling a portable device to access encrypted music on a memory storage device comprising:

one or more application programming interfaces configured to:

receive a plurality of commands from a user interface of the portable device; and

send commands to an isolated security engine, the isolated security engine configured to:

receive commands from the application programming interface;

copy encrypted keys and encrypted content from the memory storage device to a memory of the portable device;

decrypt the keys;

decrypt the content using the decrypted keys; and thereafter

delete the decrypted keys.

24. (Currently Amended) A method for allowing a device having a processor and random access memory to easily access encrypted data from a memory card with a group of commands, the method comprising:

retrieving playlist information from the memory card and storing the information in the random access memory of the device;

retrieving track information from the memory card and storing the track information into the random access memory of the device;

receiving a command selected from the group of commands from the device, the command accessing both of the playlist information, and track information from the random access memory; and

executing the command by retrieving the encrypted data stored within the memory card and decrypting the data based on the accessed information, wherein decrypting the data comprises,

(a) calculating a media unique key; and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; and thereafter

(c) decrypting a group of frames comprising less than an entire track; and thereafter

(d) deleting the decrypted title key;

(e) deleting the media unique key; and

(f) repeating (a) through (e) until the entire track is completed.

25. (Original) The method of claim 24 wherein the playlist information comprises:

the name of a playlist;

the playlist name string length;

the playback time of the playlist;

the tracks comprised by the playlist; and

the index corresponding to the playlist.

26. (Original) The method of claim 24 wherein the track information comprises:

a track number;

an index corresponding to the track number;

a number of track units in the track; and

the playback time of the track.

27. (Original) The method of claim 24 wherein the track information comprises:

a format type of a track;

a sampling frequency of the track;

the size of the track in bytes; and

the current track being decrypted.

28. (Original) The method of claim 27 wherein the general track information further comprises:

the number of audio objects comprised by the track;

the first audio object comprised by the track;

the last audio object comprised by the track;

the current audio object being decrypted; and

the offset of the current audio object.

29. (Original) The method of claim 27 wherein decrypting the data comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device;

copying encrypted audio or video content from the memory card into a memory buffer of the device;

decrypting one or more of the copied encrypted keys;

decrypting the copied encrypted audio or video content with the one or more decrypted keys.

30. (Canceled)

31. (Previously Amended) A software system stored on a device that enables the device to access content on a secure medium comprising:

one or more user interface modules for receiving commands from the device;

an applications programming interface for receiving the commands from the user interface module(s) and managing the retrieval and storage of both encrypted and non encrypted content from the secure medium;

a security engine for decrypting the encrypted content and encrypted keys sent from the secure medium to memory of the device, the decrypted keys used to decrypt the encrypted content, and wherein

one or more of the keys are contained in a first encrypted data segment, and

encrypted content is contained in a second encrypted data segment, and

the security engine buffers and decrypts a portion of the first data segment, buffers and decrypts the second data segment, and thereafter deletes the decrypted one or more keys before decrypting another portion of the first encrypted data segment, such that decrypted keys are in a decrypted state for the time it takes to decrypt less than one to about five seconds of content.

32. (Original) The software system of claim 31, wherein the key is in a decrypted state for the time it takes to decrypt and process about two seconds of content.

33. (Original) The software system of claim 32, wherein the content is encoded in the form of AAC, MP3 or WMA.

34. (Original) The software system of claim 31, wherein the portion of the first data segment buffered and decrypted is about 512 bytes.